

## REMARKS/ARGUMENTS

Claims 1-44 are now pending. No claims stand allowed.

### The 35 U.S.C. §102 Rejection

Claims 1-5, 17-25, 29-32 and 41 stand rejected under 35 U.S.C. §102(b) as being allegedly anticipated by Hacherl (U.S. Pat. No. 6,324,571 B1), among which claims 1, 17, 21, 29, and 41 are independent claims. This rejection is respectfully traversed.

“A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.”

*Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). “The identical invention must be shown in as complete detail as is contained in the ... claim.” *Richardson v. Suzuki Motor Co.*, 869 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). *See also*, M.P.E.P. §2131.

Claim 1 defines a high reliability computer system. The claimed computer system comprises a first processing engine (PE), a first memory accessible by said first PE, containing initialization information for said first PE, a second PE, a second memory accessible by said second PE, containing initialization information for said second PE, a third memory accessible by said second PE, a fourth memory accessible by said second PE, circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE, and a password passer writing said

enable password of said first PE to the fourth memory accessible by said second PE, as recited in claim 1.

I. In paragraph 5 of the Final Office Action, the Examiner maintains his rejection by equating Hacherl's role owner (pre-defined master server) with the claimed first PE, Hacherl's another server to which the control of a network system (FSMO role) is transferred with the claimed circuitry and the claimed second PE, and Hacherl's "replication functionality" with the claimed automatically switching control by the circuitry. (In Hacherl, the terms "server", "domain server", "domain controller" and "controller" are used interchangeably. The terms "role", "Master role", and "FSMO role" are also used interchangeably in Hacherl.) The Examiner further alleges as follows:

It would be futile for the continuous and smooth operation of a network with a plurality of controllers, if a mechanism to detect failure of a domain controller and automatic transfer of a particular role owner to another machine when a machine which has that particular authority (such as being master domain controller) fails or crashes is not implemented. On page 17, lines 5-7, applicants argue that in Hacherl's system a system administrator manually transfers authority of domain controller from one machine to another machine. A system administrator performs this function when a controller is scheduled for maintenance or when it is deliberately planned to change the role of a machine (see, col. 11, lines 16-50 and col. 12, line 66-col. 13, line 19).

However, Applicants respectfully disagree for the following reasons:

A. Regarding Hacherl's replication functionality (column 9, line 66-column 10 line 40 thereof, as cited by the Examiner):

First, Hacherl's replication functionality (the alleged automatically switching control) requires that both of the current role owner (the alleged first PE) and the requesting server (the alleged second PE) are functioning properly, because, in Hacherl,

the requesting server issues *and the current role owner receives* a requests that a particular FSMO role be transferred from the current role owner to the requesting machine (column 10 lines 1-4 thereof, *emphasis added*). As shown in FIG. 6 of Hacherl, if, at step 122 the current role owner is *not available* to be transferred (for example, is busy or has simply crashes), a communication to that effect (i.e., the transfer request) is returned to the requesting server and the replication process ends at step 124 (column 10 lines 8-10 and 12-13 of Hacherl, *emphasis added*). The alleged replication process steps 126-132 are performed only if “the current role owner is available for transfer,” and “at step 126 the role owner attribute stored in the local copy of the directory services database located on the current role owner is updated to identify the requesting server” (column 10, lines 14-18 of Hacherl). Thus, Hacherl’s replication functionality (the alleged automatically switching control) is operable only there is no failure of the current role owner (the alleged first PE), contrary to the claimed invention.

On the other hand, the processes performed when the current role owner is not available, for example, it has been crashed, is described in column 11, lines 16-53 of Hacherl. In Hacherl, if the current role owner is not available, the FSMO role transfer (the alleged automatically switching control) “is *not appropriate* and role seizure is necessary” (column 11, lines 16-17 thereof, *emphasis added*). That is, Hacherl’s “role seizure” is not a function performed “when a controller is scheduled for maintenance or when it is deliberately planned to change the role of a machine,” as the Examiner alleges, but that performed when a role-owner controller is crashed, goes off-line, or otherwise unavailable. As described in column 11, lines 18-20 and 40-44 of Hacherl, if the current

role owner (controller 110a) is not available (goes off-line or crashed), it is necessary to promote another domain controller (controller 110b) to role owner for continued system operation. Thus, a system administrator, logged on from the controller 110c, issues a command to the controller 110c to seize the Master role (column 11, lines 22-24 and 44-47 of Hacherl). In response to the command, the role owner attribute on the controller 110c (local copy 112c) is immediately updated to identify controller 110c as the role owner (column 11, lines 24-27 and 47-50 of Hacherl). Thereafter, the remaining local copies 112b and 112d on other controllers 110b and 110d are updated via scheduled replication procedures (column 11, lines 27-31 and 51-53 of Hacherl). Thus, in Hacherl, a system administrator's intervention is necessary for "continued system operation" in the case where the current role owner crashes or becomes unavailable.

Accordingly, the FSOM role transfer using replication functionality (the alleged automatically switching control) is operable in Hacherl only when the current role owner is available for transfer. If the current role owner is not available (crashes), the replication functionality is used only after the Master role has been manually transferred to the new controller 110c, and the role owner attribute (update) is replicated such that the remaining servers (110b and 110d) identify the new role-owner controller 110c.

Therefore, the replication functionality (the alleged automatically switching control) is performed only when there is no crash or failure of the current role owner (the alleged first PE), and when the current role owner crashes, the alleged switching is not performed automatically, but performed manually by a system administrator through a

new controller. Accordingly, Hacherl fails to disclose the claimed circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE, as recited in claim 1.

**B. Regarding the following Examiner's allegation:**

It would be futile for the continuous and smooth operation of a network with a plurality of controllers, if a mechanism to detect failure of a domain controller and automatic transfer of a particular role owner to another machine when a machine which has that particular authority (such as being master domain controller) fails or crashes is not implemented.

Applicants respectfully submit that the Examiner's allegation is incorrect for the following reason:

As discussed above, the alleged continuous operation of Hacherl's system requires a system administrator's intervention if the current role owner crashes. There is no automatic transfer in Hacherl upon the master role owner's failure. It is Applicants' disclosure that provides "a mechanism to detect failure of a domain controller and automatic transfer of a particular role owner to another machine when a machine which has that particular authority (such as being master domain controller) fails or crashes." Hacherl only discloses or teaches the allegedly smooth control transfer only when the master controller is available (without crash or failure), and the alleged continuous and smooth operation of a computer system upon failure of a first PE is only found in Applicants' own disclosure. Knowledge of applicant's disclosure must be put aside in reaching this determination, and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. M.P.E.P. § 2142. That is, the references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention.

*Hodosh v. Block Drug Co., Inc.*, 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986).

II. In paragraph 6 of the Final Office Action, the Examiner further alleges that Hacherl discloses the claimed password passer, citing column 5, lines 25-35, column 9, lines 20-23, column 3, lines 16-19, and column 8, lines 53-59 thereof. However, Applicants disagree for the reasons set forth below.

In Hacherl, the “replica” is a *replica of directory* maintained by a corresponding domain controller (column 5, lines 14-18 thereof, *emphasis added*). Hacherl’s directory service provides a logically centralized location for finding shared resources such as an e-mail server, address book, DNS, print server, database server, security server, http server, etc. in the network (FIG. 3, column 5, lines 59-66 of Hacherl, also see column 5, line 66-column 6, line 41 for detailed explanation of the directory service). That is, the directory is the information of the locations of resources in the network, not internal configuration information or enable password of the domain server itself. In general, “directory” is “[i]n network, a database of network resources, such as email addresses,” and “directory service” is “[a] network service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers” (Random House Webster’s Computer & Internet Dictionary, Third Edition, Margolis, 1999). As is well understood by one of ordinary skill in the art, an enable password which provides a privileged-mode access, not an ordinary user access, to a specific server, machine, or processing engine, is no way

considered as network resources which is to be made accessible to general users and applications. There is no mention in Hacherl that its domain replica (112a, 112b, 112c, or 112d) includes the corresponding domain server's internal configuration information or enable password. Column 5, lines 25-35 of Hacherl merely explains that each domain controller has its own replica (writable copy) of the directory, which is updated using the directory replication system discussed above.

Citing column 3, lines 16-19 and column 8, lines 53-59 of Hacherl, the Examiner also alleges that the role owner attribute which is stored in a server database includes the enable password which is replicated to other servers. However, this is not correct for the following reasons.

As is clearly described in column 8, lines 54-55 of Hacherl, "the role owner attribute *for identifying the current FSMO role owner* is stored in the *directory service* database" (*emphasis added*). That is, the "role owner attribute" merely identifies a particular server which is the current role owner of the system, but does not provide any privileged access to that particular server. This is also clearly explained in column 2, lines 13-15 of Hacherl that the master server role owner is identified in an attribute (called, for example, "role owner") that is stored on each server in the network. That is, if the role owner attribute stored in each directory service database identifies "server 110a", the server 110a is the current master server. If the role owner is transferred to the server 110c for some reason, the role owner attribute is updated to "server 110c" such that every server knows now the server 110c is the master server.

This is also in accordance with an ordinary meaning of an “attribute,” which is defined as follows:

1. A characteristic. ... In database systems, a field can have various attributes. For example, if it contains numeric data, it has the *numeric attribute*. 2. In database-management systems, the term *attribute* is sometimes used as a synonym for *field*. ... (Random House Webster’s Computer & Internet Dictionary, Third Edition, Margolis, 1999, *emphasis* original.)

Thus, according to the ordinary meaning, the role owner attribute should be a database field which contains “role owner.” Such a role owner attribute as a simple role-owner identifier should not include an enable password of the master server, since, if so, any server or user can obtain the privileged access to the master server just as knowing the master server, and can make changes, which might be destructive, to the master server configuration, or reboot, reset the master server. Providing an enable password with or as the master role owner identification would destroy the very security purpose of setting the enable password and providing a privileged access mode in any computer system.

Accordingly, the role owner attribute of Hacherl should not include any enable password of the role owner, and thus Hacherl also fails to disclose a password passer writing said enable password of said first PE to the fourth memory accessible by said second PE, as recited in claim 1.

In addition, column 9, lines 18-23 of Hacherl describes as follows:

In prior versions of “WINDOWS NT®”, clients always performs certain tasks at



one domain controller, the primary domain controller (PDC). For instance, changing a password in earlier version of "WINDOWS NT®" involves communicating with the PDC.

Thus, "changing a password" is one of the tasks which the clients performs at the PDC. That is, the entity that changes a password and communicate with the PDC is the client, not the PDC (master server). The password changed here is a client's log-in password, not an enable password or any other password of the PDC or master server. It should be noted a client cannot be a domain controller as shown in FIG. 2 of Hacherl.

Furthermore, in Hacherl, when the current role owner **110a** crashes, or otherwise unavailable, a system administrator has to log onto a different, to-be-the-role-owner controller **110c**, not the crashed controller **110a**, as discussed above. Since an enable password which allows privileged access (such as changing configuration) is set for each controller for security reasons, as is well understood by one of ordinary skill in the art (i.e., no system administrator would set the same enable password for different controllers), the system administrator does not need the enable password of the crashed controller **110a** when logging onto a different controller **110c**. Accordingly, Hacherl does not provide any motivation or desirability to make an enable password of the current role owner **110a** (the alleged first PE) accessible by another controller **110c** (the alleged second PE).

Claims 17, 21, 29, and 41 also include, among others, substantially the same distinctive feature as claim 1. Accordingly, it is respectfully requested that the rejection

of claims based on Hacherl be withdrawn. In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

The First 35 U.S.C. §103 Rejection

Claims 6-16, 26-28, 33-39 and 42 stand rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hacherl (U.S. Pat. No. 6,324,571) in view of Kung (U.S. Pat. No. 5,241,594) over the admitted prior art, among which claims 6, 12, 16, 26, 28, 33, 38 and 42 are independent claims. This rejection is respectfully traversed.

According to M.P.E.P. §2143,

To establish a *prima facie* case of obviousness, three basic criteria must be met. First there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure.

Furthermore, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).

Claim 6 defines a high reliability computer system. The claimed system comprises a first PE, a first memory accessible by said first PE, containing initialization information for said first PE, a second memory accessible by said second PE, containing initialization information for said second PE, circuitry for automatically switching control

of said system from said first PE to said second PE upon detection of a failure of said first PE, a password memory accessible by said first and second PEs, having a location for storing an enable password for the system, and a password keeper for maintaining said enable password in said password memory for said first and second PEs, as recited in claim 6.

As discussed above in response to the §102 rejection, Hacherl does not teach or suggest circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE, as also recited in claim 6. The Examiner only cites Kung for allegedly teaching a password keeper and a password server (the Final Office Action, page 4, paragraph 7), and Kung does not teach or suggest the missing features of the claimed circuitry for automatically switching control. Therefore, Hacherl, whether considered alone or combined with or modified by Kung, does not teach “circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE,” as recited in claim 6.

Claims 12, 16, 26, 28, 33, 38 and 42 also include, among others, substantially the same distinctive feature as claim 6. Accordingly, it is respectfully requested that the rejection of claims based on Hacherl and Kung be withdrawn. In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

The Second 35 U.S.C. §103 Rejection

Claims 40 and 43-44 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hacherl in view of Alonso et al (6,434,700 B1). This rejection is respectfully traversed.

Claim 40 defines a program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for providing password protection for a high reliability computer system. The system including a first PE, a first memory accessible by said first PE, said first memory containing initialization information for said first PE, a second PE, a second memory accessible by said second PE, said second memory containing initialization information for said second PE, and circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE, as recited in claim 40. The claimed method comprises (a) sending an enable password for the high reliability computer system for storage in a database of a password server coupled to the high reliability computer system via an information bus, (b) providing an interface capable of communicating with the password server over the information bus, and (c) obtaining the enable password from the password server through the interface in response to a request from either one of the first and second PEs, as recited in claim 40.

As discussed above in response to the §102 rejection, Hacherl does not teach or suggest the circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE, as also recited in claim 40.

In the Office Action, the Examiner only cites Alonso for allegedly teaching an AAA server to store an enable password in a database and authenticating the users attempting to access resources on the network and recited in claim 40 (the Final Office Action, page 5, paragraph 7). Similarly to Kung, Alonso also fails to teach or suggest the circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE. Therefore, Hacherl, whether considered alone or combined with or modified by Alonso, does not teach “circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE” as recited in claim 40.

Claims 43 and 44 also include, among others, substantially the same distinctive feature as claim 40. Accordingly, it is respectfully requested that the rejection of the claims based on Hacherl and Alonso be withdrawn. In view of the foregoing, it is respectfully asserted that the claim is now in condition for allowance.

#### Dependent Claims

Claims 2-5 depend from claim 1, claims 7-11 depend from claim 6, claims 13-15 depend from claim 12, claims 18-20 depend from claim 17, claims 22-25 depend from claim 21, claim 27 depends from claim 26, claims 30-32 depend from claim 29, claims 34-37 depend from claim 33, and claim 39 depends from claim 38. The dependant claims include the limitations of the base claim. The argument set forth above is equally applicable here. The base claims being allowable, the dependent claims must also be allowable at least for the same reasons.

In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Response is earnestly solicited.

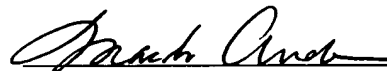
If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Please charge any additional required fee or credit any overpayment not otherwise paid or credited to our deposit account No. 50-1698.

Respectfully submitted,  
THELEN REID & PRIEST, LLP

Dated: June 1, 2004



Masako Ando

Limited Recognition under 37 CFR §10.9(b)

Thelen Reid & Priest LLP  
P.O. Box 640640  
San Jose, CA 95164-0640  
Tel. (408) 292-5800  
Fax. (408) 287-8040